FOR OFFICIAL USE ONLY

ACQUISITION SENSITIVE

Army Cloud Computing Enterprise Transformation (ACCENT)

Performance Work Statement (PWS)

August 2016

PREPARED BY:
Deputy Product Lead, Enterprise Computing

Table of Contents

I. Introduction

Product Lead, Enterprise Computing (PL EC) seeks qualified Contractors to provide commercial cloud service offerings and Information Technology (IT) technical support for transition of Army enterprise system/applications migrating to a commercial cloud environment or an Army Enterprise Hosting Facility (AEHF). These requirements are in support of the Army Data Center Consolidation Plan (ADCCP) modernization and migration requirements. The Army is moving designated IT applications, systems and associated data to authorized commercial cloud service providers (CSP) and consolidating data centers to AEHF.

Basic Ordering Agreements (BOAs) will be issued to allow Army capability owners to obtain commercial cloud hosting services in any combination of service models, deployment models, and Impact Levels as defined in the DoD Cloud Computing Security Requirements Guide (CC SRG) along with transition support services required to move a system/application to a cloud environment. Cloud requirements may also include mobile computer solutions. The ACCENT BOA will be the Army's preferred source used by all Army commands and organizations requiring commercial cloud hosting, data center migration, transition support, and application modernization services.

II. Background

In May 2011, the Army issued the Army Data Center Consolidation Plan (ADCCP) Execute Order requiring the Army to consolidate hundreds of Army data center facilities into standardized Core Data Centers (hereafter referred to as AEHF) and move enterprise systems and applications to Defense Information Systems Agency (DISA) or to commercial cloud hosting services authorized by the Department of Defense (DoD). The Army Cloud Computing Strategy provided additional guidance to include Army applications that should be migrated to DoD-authorized government and commercial Cloud Service Offerings (CSOs) if doing so aligns with mission requirements without compromising security. The ADCCP requires Army commands, staff, mission areas and domain managers to review the Army's portfolio of applications and issue disposition decisions to sustain, kill, or modernize applications. The enduring applications will be migrated to authorized AEHF or commercial cloud hosting environments.

To implement the ADCCP, the Army Cloud Computing Strategy, issued March 2015, formalized the Army's strategy for leveraging cloud computing to improve effectiveness and increase efficiency at reduced cost. On 10 August 2015, the Army Chief Information Officer (CIO)/G-6 issued the "Guidance for Migration to, and Use of, Commercial Cloud Service Providers (CSPs)" requiring the Army to migrate enterprise-level capabilities to cloud hosting environments authorized by the DoD. To implement Army Cloud Computing Strategy, the Army will procure commercial cloud services from CSPs for authorized CSOs. To ensure cost effective cloud solutions and continuity of service, the Army will also procure transition support services (including associated application modernization services) as appropriate.

III. Scope

The ACCENT scope includes services and solutions necessary for the Army to satisfy the requirement for migration of eligible Army enterprise applications to commercial cloud service providers and to AEHFs. Commercial cloud services will be acquired based on approved Cloud Service Provider (CSO) Cloud Service Offerings (CSOs) (i.e., those with a DoD Provisional Authorization). ACCENT will also enable capability owners to modernize and transition applications to CSP/CSOs and AEHFs,and facilitate the acquisition of modular or mobile hosting facilities.

Cloud Computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. Cloud computing solutions include the Infrastructure as a Service (IaaS), Platform as a Service (PaaS), or Software as a Service (SaaS) cloud service models, and the Private, Community, Public, and Hybrid deployment models (as applicable). Cloud hosting solutions may require either on-premise or off-premise hosting, and support hosting of systems/applications at Information Impact Levels 2, 4, 5, or 6. CSP may be required to maintain operations 24 hours a day, seven days a week. These characteristics are more fully defined in the CC SRG.

The Government intends to leverage existing enterprise licenses to the extent possible. If applicable, task orders (TO) will identify enterprise licenses that the Government intends to use within the IaaS and PaaS cloud service models as Government Furnished Property. The Government will specify who is responsible for acquiring, tracking, provisioning, and ensuring compliance for license management in the TO.

The volume of TOs issued under the ACCENT BOA will be dependent upon the number of Army enterprise applications transitioning to the commercial cloud or an AEHF. There are approximately 10,000 known applications; however, not all of these applications will be identified as viable applications to migrate. Transition and hosting needs will likely grow substantially as the Army consolidates data centers and identifies applications that are candidates to be migrated to the commercial cloud or AEHF.

The Contractor teams will be required to provide solutions pursuant to the cloud characteristics discussed below. Specific and detailed requirements will be identified in individual TOs. All services performed under ACCENT shall be performed in accordance with (IAW) best commercial practices and Government standards, regulations, as described herein and within each TO. If any of the practices, standards or regulations conflict, the more rigorous requirement will take precedence. Each TO will specify required capability performance specifications and parameters for the operation of the Government's capability. The objective is to ensure effective operation of the capability following migration to the Contractor's cloud environment.

III.a. Commercial Cloud/AEHF Hosting and Transition Support Services

TOs will define the systems/applications being transitioned from the current operational environments to the CSP/CSO or AEHF. Following TO award, the Contractor teams shall work with the capability owning organization to perform the activities required to prepare the capabilities for migration and support transition to the cloud hosting environment.

III.a.1 Transition Support Services:

Cloud transition support activities may include application analysis, security requirements analysis, documentation, modernization (code refactoring and augmentation), virtualization, technical engineering, migration scheduling, business process reengineering, data preparation, migration planning, interface transition planning, training on CSO environment, service transition planning, cutover planning, back out planning, and go-live support.

Application modernization may be required as part of transition support services. Modernization is the refactoring or consolidation of legacy software programming to align it more closely with current business needs. In this case, modernizing systems/applications to migrate to

commercial cloud hosting environments. The Contractor shall work with capability owners to modernize systems/applications to transition them from current operating environments to a CSP/CSO or AEHF. TOs will define the systems/applications being modernized and moved from current operational environments to the CSP/CSO or AEHF. Following TO award, the Contractor shall work with the Government to perform the activities required to prepare the capabilities for migration and support transition to the cloud hosting environment.

The following are core activities performed in application modernization activities.

- Develop application documentation to support modernization or improve maintenance and testing efficiency.
- Identify approaches to modernize and upgrade applications to enhance business value.
- Consolidate and rationalize data and applications to eliminate redundancy, improve efficiency and make improvements to data quality.
- Enhance security to latest standards of best practice and compliance.
- Re-architect applications to leverage modern architecture standards and interface capabilities.
- Assess, plan and implement server workload consolidations to reduce cost and complexity while migrating to a modernized and scalable platform.

III.a.2 Cloud Hosting Services:

The Contractor teams will provide the cloud hosting services in accordance with the DoD PA they have received for their CSO. General characteristics and attributes for IaaS, PaaS and SaaS cloud service models are summarized below. Specific requirements will be defined in TOs.

IaaS:

- Allow the cloud service customer to provision and use processing resources (central processing unit, random access memory, and storage) via, for example, an on demand web-based portal, to perform operations relevant to VM lifecycle operations, such as VM reboot, shut down, migration, backup, snapshot, clone, and reservation
- Allow the cloud service customer to view and configure metric data about VMs and allow the configuration of thresholds and alerts
- Provide x86-architecture based computing resources capable of hosting/installing industry standard operating systems on virtual machines
- Allow the cloud service customer to use virtual networking resources and perform virtual network functions such as Internet Protocol (IP) address, subnets/Virtual Local Area Networks (VLANs), routers, switches, load balance, and firewall to enable the creation of virtual networks between VMs such as isolated user, management, or data planes
- Provide an infrastructure that is Internet Protocol version 6 (IPv6) enabled and support Internet Protocol version 4 (IPv4) legacy applications
- Provide Virtual Private Network (VPN) services to enable access to IaaS resources via a VPN connection from an on-premise location

- Allow the attachment of storage at various tiered performance levels to accommodate use cases such as archival-quality storage and high-performance storage
- Provide an Application Programming Interface (API) for VM provisioning and management
- Provide options to synchronize/replicate a different data center when backup services are provided. The cloud service customer shall be able to select/configure backup services, including selection of backup locations, frequency of backups, and attributes of the backup (incremental, differential, full, application and database support, encryption, etc.), including backup versioning
- Services for monitoring the health and status of the VMs shall be available in near real-time, including VM operational status, VM uptime, and VM resource status (configured resources, used resources, maximum resources available). Trending and other historical usage shall also be made available
- Follow FedRAMP and DoD PA guidelines to keep the IaaS infrastructure fully patched against known vulnerabilities

PaaS:

- The services and tools provided in a PaaS environment shall streamline the development and deployment of cloud-enabled/cloud-optimized applications
- The tools and software components provided in the PaaS CSO shall be kept patched and up-to-date IAW with articulated Army and DoD standards
- A process or mechanism shall be available to the consumer to allow upgrading from one version of the PaaS CSO to a newer (patched) version of the CSO with minimal/managed disruption to the hosted application
- The PaaS layer shall provide the automation of provisioning, configuration, and adminstration of the underlying PaaS resources
- The PaaS layer shall provide support for multiple environments including, but not limited to, development, development test, testing, staging, production
- The PaaS layer shall provide support for a variety of program languages, such as Java, Python, Ruby, ASP.NET, Node.js, PHP, etc.
- The PaaS layer shall provide support for a variety of server types, such as Application Server, Java Enterprise Edition Container, Web Server, .NET Server and Ruby Application Server
- The PaaS layer interface shall allow authorized Application Developers to upload compiled code (e.g., a .war file or .NET library) into the PaaS layer. This may be a web based user interface, or ideally, be integrated with popular Integrated Development Environments (IDEs)
- The PaaS layer shall include an IDE Toolkit. This is a toolkit that integrates with one or more IDEs
- The IDE toolkit should give an authorized developer the ability to deploy an application into the cloud development environment
- The PaaS environment shall include support for various build tools, such as Maven or Ant

- The PaaS environment shall offer a continuous integration tool, such as Jenkins or Hudson
- A version control system shall be available to developers
- A Configuration Management tool shall be made available to developers. The tool(s) shall include the ability to deploy, configure, and patch an application. The tool(s) shall work with the development environment and link into the version control system
- At least one relational database service shall be provided that supports Structured Query Language. It is preferred that both an open source database as well as a commercial database be offered. At least one of the databases shall offer support for geospatial queries
- Follow FedRAMP and DoD PA guidelines to keep the PaaS infrastructure fully patched against known vulnerabilities

SaaS:

- Manage and control all of the underlying cloud infrastructure, operating systems, application platforms and capabilities
- Ensure application and data availability, performance, and durability meet or exceed thresholds defined by capability owner requirements
- Allow cloud service customers to export all of their data from the SaaS CSO at any time, as well as the capability to import/re-import data to the SaaS CSO
- Follow FedRAMP and DoD PA guidelines to keep the SaaS environment fully patched against known vulnerabilities.

III.b. Cloud Hosting in Off-Premise and On-Premise Environments:

Contractor teams may be required to provide cloud computing in either an on-premise or off-premise environment. In these environments, ownership and operation of cloud computing service, to include operating environment, real estate, and capital equipment can be either Contractor Owned Contractor Operated (COCO), Government Owned Contractor Operated (GOCO), Contractor Owner Government Operated (COGO), or Government Owned Government Operated (GOGO).

III.b.1 Off-Premise:

To protect against seizure and improper use by non-US persons and government entities, all data/information stored and processed by/for the DoD must reside in a facility under the exclusive legal jurisdiction of the US. CSPs will maintain government data that is not physically located on DoD premises within the 50 States, the District of Columbia, and outlying areas of the US (as defined at FAR 2.101), unless otherwise authorized by the responsible Authorizing Official (AO), as described in DoDI 8510.01. The contracting officer shall provide written notification to the contractor when the contractor is permitted to maintain Government data at a location outside the 50 States, the District of Columbia, and outlying areas of the United States. CSPs shall provide a list of the physical locations where the data would be stored at any given time and update that list as new physical locations are added.

III.b.2 On-Premise:

On-premise includes DoD data centers or other facilities located on a DoD Base/Camp/Post/Station (B/C/P/S), or in a commercial or another government facility (or portions thereof) under the direct control of DoD personnel and DoD security policies. A commercial facility, in this sense, means a building or space leased and controlled by DoD. Physical facilities may be permanent buildings or portable structures such as transit/shipping containers. An example of the latter might be a container housing a commercial CSP's infrastructure located adjacent to a data center and connected to its network as if it was inside the building.

CSPs may instantiate their cloud service architecture on DoD premises. Interconnection with DoD networks will be interoperable IAW engineering requirements that meet cybersecurity guidance and controls. Such implementations will be considered DoD Private.

On-premises CSOs implemented by a CSP which utilizes a hybrid model employing off-premises CSPs and CSOs to augment the on-premises CSO must be able to meet the location requirements stated in CC SRG "Section 5.2.1.1: Jurisdiction/Location Requirements for DoD Off-Premises Locations."

In the provision of fixed on-premise and off-premise data centers the contractor shall have the capability to:

- Provide, maintain, operate, and support data centers providing virtualized capacity to Army application owners;
- Perform data center management tasks;
- Perform required physical and environmental security measures;
- Provide hardware and software necessary for integration, implementation, and operation of army applications and systems;
- Provide a cloud service offering that is FedRAMP and DoD PA certified.

III.c. Cloud Hosting in Mobile Data Centers:

The contractor teams may be required to provide, maintain, operate, and support mobile data centers, thereby supplying virtualized operating environments and resource capacity to application owners. If necessary, the contractor shall provision and deliver cloud hosting services in a mobile, containerized data center format. The contractor shall have the requisite engineering, transportation, and logistics expertise related to design and appropriate sizing and transportation of mobile data centers. All policy, security and technical requirements identified in other sections of the PWS will be applicable, as required, for mobile data centers. Task Orders will provide contractors with capacity and operating environment requirements and contractors will propose the appropriate container size to meet the requirements. The contractor shall provide mobile data center hardware and software necessary for integration, implementation, and operations of identified Army applications and systems. The contractor shall provide on-site support for the mobile data center.

IV. General Provisions

Contractor teams will be required to adopt and maintain security (management, operational, technical) and privacy requirements for their CSO impact level and cloud service model being

provided, in accordance with FedRAMP and the CC SRG. If security controls/requirements for the DoD PA change, contractors will comply with the changes to retain their DoD PA.

The Contractor shall be compliant with the security standards required to maintain the following authorizations and requirements:

The Contractor shall continue compliance with FedRAMP including all federal laws, directives, policies, FIPS standards, NIST guidance, and security requirements identified in the FedRAMP Moderate baseline security controls.

ACCENT BOAs will only be executed with a Contractor team who has a DoD PA for the CSO(s) being proposed. The Contractor shall have a DoD PA for all CSOs being provided under its ACCENT BOA IAW the CC SRG (Section 4.3) which states, "Each CSO must be granted a DoD PA in order to host DoD mission systems."

APPENDIX A: REFERENCED REQUIREMENTS DOCUMENTS

Applicable documents cited throughout this PWS defining compliance or required action are identified below. All applicable documents will be cited as necessary in individual TOs. The CC SRG is being updated and may be updated annually. The CSP must remain in compliance with the latest published CC SRG in accordance with FedRAMP and DoD annual assessment processes.

Reference document number:

1. DoD Cloud Computing Security Requirements Guide, Version 1, Release 2, 18 MAR 2016
2. NIST Special Publication 800-145
3. Army Chief Information Officer (CIO)/G-6, “Guidance for Migration to, and Use of, Commercial Cloud Service Providers (CSPs),” 10 August 2015
4. Army Chief Information Officer/G-6, Army Cloud Computing Strategy, March 2015
5. Army Data Center Consolidation Plan (ADCCP)
6. Army Regulation (AR) 25-2, Information Assurance, 23 March 2009
7. AR 381-12, Threat Awareness and Reporting Program, 04 October 2010
8. AR 530-1, Operations Security, 26 September 2014
9. Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01B, Cyber Incident Handling Program, 18 December 2014
10. Committee on National Security Systems Instruction (CNSSI) 1253, Security Categorization and Control Selection for National Security Systems (CNSS), 27 March 2014
11. CNSSI 4009, Committee on National Security Systems (CNSS) Glossary, 06 April 2015
12. DoD 5200.01-R, DoD Information Security Program, 24 February 2012
13. Department of Defense Instruction (DoDI) 1000.13, Identification (ID) Cards for Members of the Uniformed Services, Their Dependents, and Other Eligible Individuals, 23 January 2014
14. DoDI 8500.2, Information Assurance (IA) Implementation, 06 February 2003
15. NIST SP 800-53; Security and Privacy Controls for Federal Information System and Organizations, Revision 4, April 2013
16. NIST SP 800-145, The NIST Definition of Cloud Computing, September 2011
17. Office of Management and Budget Memorandum (OMB M)-11-11, Continued Implementation of Homeland Security Presidential Directive (HSPD) 12-Policy for a

Common Identification Standard for Federal Employee and Contractors, 3 February 2011

18. OMB M-07-19, FY 2007 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management, 25 July 2007
19. Army Regulation 25–1, "Army Information Technology" dated 25 June 2013
20. DoD Instruction 8510.01, "Risk Management Framework (RMF) for DoD Information Technology dated 24 May 2016
21. The Privacy Act of 1974, 5 U.S.C. § 552v (2015 Edition)

APPENDIX B: ACRONYMS

Abbreviation	Term
ACCENT	Army Cloud Computing Enterprise Transformation
ACC-RI	Army Contracting Command – Rock Island
ADA	Anti-Deficiency Act
ADCCP	Army Data Center Consolidation Plan
API	Application Programming Interface
AR	Army Regulation
AT	Antiterrorism
ATCTS	Army Training Certification Tracking System
ATO	Authority To Operate
BOA	Basic Ordering Agreement
CAC	Common Access Card
CC SRG	Cloud Computing Security Requirements Guide
CFR	Code of Federal Regulations
CI	Counterintelligence
CIO	Chief Information Officer
CJCSM	Chairman of the Joint Chiefs of Staff Manual
CLIN	Contract Line Item Number
CND	Computer Network Defense
CNDSP	Computer Network Defense Service Provider
CNSS	Committee on National Security Systems
CNSSI	Committee on National Security Systems Instruction
COB	Close of Business
CONOPS	Concept of Operations
COR	Contracting Officer’s Representative
CPFF	Cost-Plus-Fixed-Fee
CR	Cost-Reimbursable

Abbreviation	Term
CSO	Cloud Service Offering
CSP	Cloud Service Provider
DFARS	Defense Federal Acquisition Regulation Supplement
DIB	Defense Industrial Base
DISA	Defense Information Systems Agency
DoD	Department of Defense
DoDI	Department of Defense Instruction
FAR	Federal Acquisition Regulation
FedRAMP	Federal Risk and Authorization Management Program
FFP	Firm-Fixed-Price
FOIA	Freedom of Information Act
FP	Fixed-Price
FY	Fiscal Year
HSPD	Homeland Security Presidential Directive
IA	Information Assurance
IaaS	Infrastructure as a Service
IAW	In Accordance With
ID	Identification
IDE	Integrated Development Environment
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IT	Information Technology
JIE	Joint Information Environment
LE	Law Enforcement
LH	Labor Hours
MB	Megabyte

Abbreviation	Term
NACI	National Agency Check with Inquiries
NDA	Non-Disclosure Agreement
NIST	National Institute of Standards and Technology
NLT	No Later Than
OCI	Organizational Conflict of Interest
OCOR	Order Contracting Officer's Representative
OMB M	Office of Management and Budget Memorandum
OPSEC	Operations Security
OT	Order Transaction
PA	Provisional Authorization
PaaS	Platform as a Service
PIV	Personal Identity Verification
PL EC	Product Lead, Enterprise Computing
POC	Point of Contact
PoP	Period of Performance
QASP	Quality Assurance Surveillance Plan
RFP	Request for Proposal
RMF	Risk Management Framework
SaaS	Software as a Service
SLA	Service Level Agreement
TARP	Threat Awareness and Reporting Program
TO	Task Order
US-CERT	United States Computer Emergency Readiness Team
VLANs	Virtual Local Area Networks
VPN	Virtual Private Network

APPENDIX C: CLOUD COMPUTING DEFINITIONS

Abbreviation	Term
On-demand self-service	A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.
Broad network access	Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).
Resource pooling	The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, and network bandwidth.
Rapid elasticity	Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.
Measured service	Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.
Cloud Service Models	
SaaS	The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.
PaaS	The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.
IaaS	The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).
Cloud Deployment Models (The following Deployment Models are in scope of the ACCENT BOA):	

Abbreviation	Term
Private cloud	A cloud infrastructure provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on- or off-premises. For the purposes of ACCENT, private cloud solutions can correspond to either commercial cloud (Lot 2) or AEHF (Lot 3) solutions provided in either an on-premise (physically on a DoD Base/Post/Camp/Station (B/C/P/S) in accordance with the DoD Security Requirements Guide (SRG) 5.2.1.2) facility or off-premise (in accordance with DoD Security Requirements Guide (SRG) 5.2.1.1) facility:
Community cloud	A cloud infrastructure provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises. The Community Cloud model corresponds to commercial cloud service providers with a Cloud Service Offering (CSO) that has a valid FedRAMP and DoD Provisional Authorization.
Public cloud:	A cloud infrastructure provisioned for use by the general public. It exists off-premise in a commercial cloud environment.
Hybrid cloud	A cloud infrastructure composed of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).”